Architectures for Quantum Local Area Networks (QuLAN)

ABSTRACT

Quantum Key Distribution (QKD) is an unconditionally secure method of distributing keys in a network configuration. This paper examines the implementation of key distribution in a 4-node network and tries to quantify where performance improvements and degradations might occur.

Architectures for Quantum Local Area Networks (QuLAN)

We examine the implications of extending the quantum distributing keys from a two-node LAN to a multi-node land. Instead of trying actively route qubits to control their distribution among multiple nodes, we chose to use passive switching (fiber Y-couplers). We set up an N-node network (with N=4 as in Figure 1) with each node capable of injecting a qubit and each node, except node-1 (Alice) capable of passively coupling the qubit out. Any qubits still left in the network after one cycle are automatically detected by Alice. Thus each qubit has a probability amplitude , α_i, of staying in the network and a probability, β_i, of coupling out to be analyzed and detected at the *ith*-node for all nodes except node-1.

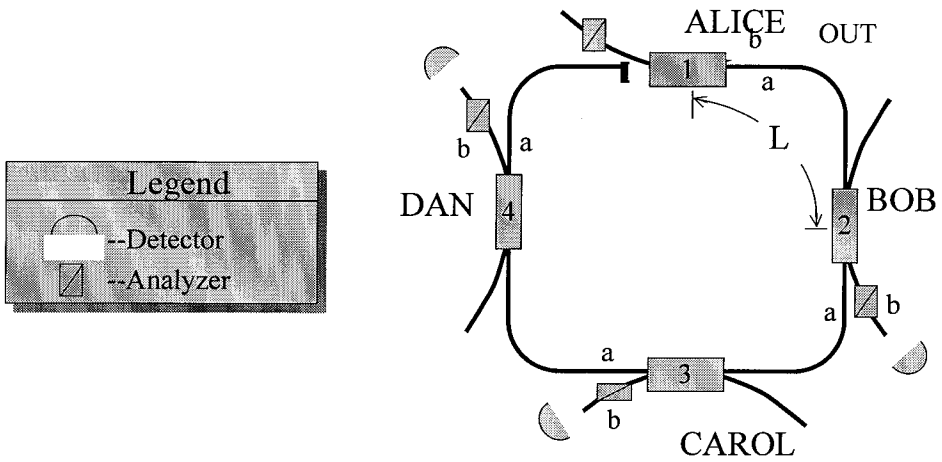

Figure 1. Notional 4-node network

By setting all of the inter-node distances are equal to the same distance, L, one can write an expression for the qubit wavefunction that describes the behavior at each node.

$$|\Psi\rangle = |\Psi(t_0)\rangle_1 + |\Psi(t_1 = t_0 + L/c)\rangle_2 + |\Psi(t_2 = t_0 + 2L/c)\rangle_3 + |\Psi(t_3 = t_0 + 3L/c)\rangle_4$$

The wavefunction reflects not only the projective measurements from Alices', Bob's, Carol's, and Dan's analyzers, but also the path uncertainty at the passive waveguide splitter. This has interesting application implications.